Lecture 11 RSA § 3.1 & 3.2.

RSA = Rivest - Shamir - Adleman

First discovered by British intelligence Clifford Cocks.

Public key Exchange

DH key exchange

RSA key exchange

HARD problem

DLP solve $g^x \equiv h \pmod p$

Solve $x^e \equiv h \pmod N$

easy if we've factored N.

$\Uparrow$

factorization.

Observation When $N=p$ is prime, solving $x^e \equiv h \pmod p$ is easy.

Solutions do not always exist.

Ex $p=5$, $e=2$

x	1	2	3	4
x^e	1	4	4	1

$\Rightarrow$ no soln to $x^2=2$ or $x^2=3$ mod 5.

Prop 1 If e & $p-1$ are relatively prime, there exists a unique $x \in \mathbb{F}_p^\times$ s.t. $x^e \equiv h \pmod p$

Conversely if $\exists\ h \in \mathbb{F}_p^\times$ s.t. $x^e \equiv h \pmod p$ has a unique soln, then e & $p-1$ are relatively prime.

e & $p-1$ relatively prime $\iff$ $x^e \equiv h$ has 1 soln for all $h \in \mathbb{F}_p^\times$

e & $p-1$ rel. prime $\iff$ $x^e \equiv h$ has 0 or ≥ 2 soln for all $h \in \mathbb{F}_p^\times$

We won't prove or use this!

pf (of Prop 1) There exist $u, v \in \mathbb{Z}$ s.t.

$eu + (p-1)v = \gcd(e, p-1) = 1$ & u is unique mod p.

$x^{p-1} = 1$ so $x = x^{eu + (p-1)v} \equiv x^{eu} = h^u$.

↑ bc $x^{p-1} = 1$

is the unique soln.

Ex Solve $x^3 \equiv 2 \pmod 5$

Soln $\gcd(3, 5-1) = 1 \Rightarrow \exists!$ soln.

Find u s.t. $eu \equiv 1 \pmod{p-1}$.

$3 \cdot 3 \equiv 1 \pmod 4$. So $u = 3$ works.

Then $x = h^u = 2^3 \equiv 3 \pmod 5$.

Ex $x^2 \equiv 4 \pmod 5$ has two solns $x = 2$ & $x = 3$.

So $\gcd(2, 5-1) \neq 1$.

Now consider the case when N is composite, specifically suppose $N = pq$ is a product of two primes. How to solve $x^e \equiv h \pmod N$?

$$\mathbb{Z}/N \cong \mathbb{Z}/p \times \mathbb{Z}/q \Rightarrow (\mathbb{Z}/N)^\times \cong (\mathbb{Z}/p)^\times \times (\mathbb{Z}/q)^\times$$

$$\cong (\mathbb{Z}/p-1 \times (\mathbb{Z}/q-1)$$

↑ Chinese Remainder Thm

Every element in $\mathbb{Z}/p-1 \times \mathbb{Z}/q-1$ has order dividing $\text{lcm}(p-1, q-1) \Rightarrow$ for all $x \in (\mathbb{Z}/N)^*$,

$$x^{\text{lcm}(p-1, q-1)} \equiv 1 \pmod{N}.$$

So can solve if e is relatively prime to $p-1$ & e is relatively prime to $q-1$.

Prop If e is relatively prime to $p-1$ & to $q-1$, there exists a unique x s.t. $x^e \equiv h \pmod{pq}$.

Pf Same as proof of prop 1.

Set $M = \text{lcm}(p-1, q-1)$. B/c

$\gcd(e, p-1) = \gcd(e, q-1) = 1$, $\gcd(M, e) = 1$.

So $\exists$ u, v s.t. $eu + Mv = 1$.

$$x \equiv x^{eu+Mv} \equiv x^{eu} \equiv h^u \pmod N.$$

$\uparrow$ b/c $x^M \equiv 1$

Ex $p=3$, $q=5$, $N=15$, $\operatorname{lcm}(p-1, q-1) = 4$.

elts of $(\mathbb{Z}/N)^\times \longrightarrow$

a	1	2	4	7	11	13	14
a^2	1	4	1	4	1	4	1
a^4	1	1	1	1	1	1	1

Ex Solve $x^3 = 4 \pmod{19}$.

Find u s.t. $3u \equiv 1 \pmod 4$.

$u=3 \Rightarrow x = h^u = 4^3 = 4 \pmod{15}$.

RSA PKE

Alice

Bob

Pick private key

p, q, u

Public key

$N = pq, e$

Publish N, e →

$eu \equiv 1 \pmod{\operatorname{lcm}(p-1, q-1)}$.

Plaintext $m \in \mathbb{Z}/N$

Ciphertext $C = m^e$.

← Publish C

$m = e^u \pmod{N}$.

Rmks

- Knowing $\operatorname{lcm}(p-1, q-1)$ equivalent(?) to knowing p, q
- It is believed that breaking RSA is easier than factoring.